ORACLE

Oracle Access Management 11gR2 (11.1.2.x)
Frequently Asked Questions (FAQ)

Overview

Oracle Access Management is a complete solution designed to securely enable business transformation with mobile and social networking technologies, hybrid on-premise and cloud applications deployment, and hybrid access management deployment while preserving a seamless user experience, centralized administration, and market-leading performance and scalability.

Key Features

Cores Services

- Multiple authentication schemes
- Web single sign-on (SSO)
- Session management life cycle
- Coarse-grained authorization

Intelligent Access Management

- Context-aware (device context, geo-location, session context, transaction context)
- Content-aware (leveraging content classification)
- Risk-aware (real-time risk assessment based on context and policies)
- Context, content, and risk driven, dynamic, step-up authentication and fine-grained authorization

Adaptive Access

- Device fingerprinting
- Predictive auto-learning
- Knowledge-based authentication (KBA)
- One-time password (OTP) using SMS, email, or Oracle Mobile Authenticator (a soft token OTP mobile app)

Fraud Detection and Investigation

- Real-time and batch analysis (heuristic behavior analysis)
- Universal risk snapshot

Identity Federation

- Support for SAML 2.0, OpenID 2.0, OAuth 2.0

Mobile Security

- Client-side SDK for authentication, SSO, and delegated authorization (OAuth)
- Support for Adaptive Access features

API and Web Services Security

- Authentication, authorization
- Data format (XML, JSON) and transfer protocol translation
- XML firewalling and throttling

Cloud Security

- Access Portal (on-premise deployment to build a cloud SSO portal)

Benefits

- Scalability (support for up to 250 million user accounts).
- High availability with active-active multiple data center support.
- Dynamic, proactive security posture, avoiding the common pitfalls of reactive, static security systems.

Table of Contents

Overview 1
Key Features 1
Oracle Access Management 3
General Questions 3
License Questions 4
Certification Related Questions 5
Feature Related Questions 5
Integration Questions 7
Oracle Access Management Access Manager (Access Manager) 8
General Questions 8
Certification Questions 9
Migrations Questions 9
Oracle Access Management Mobile and Social (Mobile and Social) 12
General Questions 12
Oracle Access Management Access Portal (Access Portal) 14
General Questions 14
Oracle Adaptive Access Manager 15
General Questions 15
Oracle Enterprise Single Sign-On Suite Plus 17
General Questions 17
Oracle Access Management Identity Federation (Identity Federation) 20
General Questions 20
Oracle Access Management Security Token Service (Security Token Service) 23
General Questions 23
Oracle Web Services Manager 25
General Questions 25
Oracle Entitlements Server 26
General Questions 26
Oracle API Gateway 28
General Questions 28

Oracle Access Management

This section contains frequently asked questions regarding all services within Oracle Access Management.

General Questions

1. I am new to Oracle Access Management 11g. Where do I begin?

The latest 11g Identity and Access Management documentation can be found at

http://www.oracle.com/pls/topic/lookup?ctx=idm111220&id=homepage

In addition, the Complete and Scalable Access Management Whitepaper provides an overview of Access Management and its key functionalities. It can be found at

http://www.oracle.com/us/products/middleware/identity-management/access-management/overview/index.html

2. Where can I find Oracle Access Management 11g software downloads?

All licensable Oracle products (including Access Management 11g) can be downloaded from the Oracle Software Delivery Cloud at

https://edelivery.oracle.com/

In addition, Access Management 11g software can be downloaded for development use from Oracle Technology Network (OTN):

http://www.oracle.com/technetwork/middleware/downloads/oid-11g-161194.html

3. What are the latest Oracle Access Management releases?

- Oracle Identity and Access Management 11.1.2.2.0 was released in January 2014. It includes the following Access Management services - Access Manager, Identity Federation, Mobile and Social, Access Portal, Security Token Service, Adaptive Access Manager, Entitlements Server, Web Services Manager, API Gateway, and Enterprise Single Sign-On.
- Oracle Identity and Access Management 11.1.2.1.0 was released in April 2013. It includes the following Access Management services - Access Manager, Identity Federation, Mobile and Social, Security Token Service, Adaptive Access Manager, Entitlements Server, Web Services Manager, API Gateway, and Enterprise Single Sign-On.
- Oracle Identity and Access Management 11.1.2.0 was released in July 2012. It includes the following Access Management services - Access Manager, Identity Federation, Mobile and Social, Security Token Service, Adaptive Access Manager, Entitlements Server, Web Services Manager, Enterprise Gateway, and Enterprise Single Sign-On.
- Oracle Identity and Access Management 11.1.1.7 was released in April 2013. It includes the following Access Management products - Oracle Access Manager, Oracle Security Token Service, Oracle Adaptive Access Manager, and Oracle Entitlements Server.
- Identity Management 11.1.1.7 was released in April 2013. It includes the following Access Management products - Oracle Identity Federation, Oracle Web Services Manager, Oracle Enterprise Gateway, and an embedded Oracle Entitlements Server PDP for Oracle Fusion Middleware technologies (such as ADF, WebCenter, and SOA Suite) as well as Oracle Fusion Applications.
- Identity Management 11.1.1.6 was released in February 2012. It includes the following Access Management products - Oracle Identity Federation, Oracle Web Services Manager, Oracle Enterprise Gateway, and an embedded Oracle Entitlements Server PDP for Oracle Fusion Middleware technologies (such as ADF, WebCenter, and SOA Suite) as well as Oracle Fusion Applications.
- Oracle Identity and Access Management 11.1.1.5 was released in May 2011. It includes the

following Access Management products - Oracle Access Manager, Oracle Security Token Service, Oracle Adaptive Access Manager, and Oracle Entitlements Server.

4. How can I find out Premier and Extended Support dates for Access Management Products?

The Oracle Lifetime Support Policy across all products (including Access Management) can be found at

http://www.oracle.com/us/support/lifetime-support/lifetime-support-software-342730.html

5. What do I need to know about Support dates and patching baselines?

The My Oracle Support article 1290894.1 covers Error Correction Support Dates for Oracle Fusion Middleware products (including Access Management)

https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1290894.1

6. What if I have a question about Access Management products or have encountered an issue?

Refer to the product documentation first:

http://docs.oracle.com/cd/E37115_01/index.htm

Oracle Support offers a wide variety of useful knowledge articles related to common questions raised by customers. If the documentation does not address your question, raise a Service Request (SR) with Oracle Support at http://support.oracle.com.

License Questions

1. Where do I find pricing and licensing information?

The pricing and licensing information for all Oracle products can be found at http://www.oracle.com/us/corporate/pricing/index.html

2. What is an Oracle Access Manager Basic License and what does it mean?

The Oracle Access Manager (OAM) Basic license was created to support customers that own Oracle AS Single Sign-On (OSSO) - either through buying the Oracle iAS Suite or other products such as Oracle E-Business Suite. The OAM Basic license stipulates that a customer with valid Oracle Single Sign-On (OSSO) licenses can exchange them for an equivalent number of Access Manager licenses with some restrictions. The restrictions require the use of Oracle infrastructure components for Access Manager; this was also a requirement for OSSO. For example, the LDAP directory has to be Oracle Internet Directory or Oracle Virtual Directory and only protection of Oracle application resources are allowed. If a customer wants to remove the restrictions, they will need to purchase the full Access Manager license. For more detailed information, refer to http://docs.oracle.com/cd/E23943_01/doc.1111/e14860/oam_basic.htm#CHDBECDJ

3. What license is required to use OAuth?

OAuth is part of Access Management Federation Services. If you have licenses that include Federation, such as Oracle Identity Federation, Oracle Access Management Suite Plus, Oracle Identity and Access Management Suite Plus, are you entitled to OAuth capabilities.

4. I do not see my question about licensing answered here, what do I do?

Additional questions and answers about licensing are addressed in the Identity and Access Management Licensing Document at

http://docs.oracle.com/cd/E28280_01/doc.1111/e14860/im_options.htm

If you still not sure about your license options or have additional questions, please discuss these with your Oracle Sales Representative.

Certification Related Questions

1. Where can I find the latest information about supported configurations (including Operating Systems, Browsers and LDAP directories)?

For the latest supported 11g Access Management configurations, refer to the certification matrix available on Oracle Technology Network at:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

2. Where can I find the latest information about interoperability between Oracle Fusion Middleware 11g / 12c products and Oracle Access Management 11g products?

Refer to the Oracle Fusion Middleware 11g / 12c certification matrix for interoperability details / support with Oracle Access Management 11g products:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

Feature Related Questions

1. Oracle Access Manager, Oracle Identity Federation and other products used to be installed and managed as independent products. Has this changed in Oracle Access Management 11.1.2.x releases?

Access Manager, Identity Federation, Security Token Service, Mobile and Social, and Access Portal are installed as part of the same software bundle in 11.1.2.2.0. These services are configured via the OAM Administration Console. Note that activation of these services is allowed only if licensed.

2. Both Oracle Enterprise Single Sign-On and Oracle Access Manager provide single sign on capabilities. What is the difference between these two products?

Access Manager is a solution that provides seamless and secure access to web applications. Oracle Enterprise Single Sign-On is a solution that provides seamless and secure access to desktop, java and mainframe applications.

3. Both Oracle Access Manager and Oracle Entitlements Server have authorization capabilities, but one is coarse-grained and the other fine-grained. What is the difference between the two and where is the appropriate place to use them?

Oracle Access Manager provides (what is sometimes referred to as) coarse-grained authorization. This protects access to a given web application at the URL level. For example, can user A access application 1?

Oracle Entitlements Server (OES) provides fine-grained authorization by controlling what users can do with applications, portals, content management systems, web services and databases. For example, OES can control:

- UI widgets including menu items, tabs, portlets, fields, and buttons that can be enabled or rendered.
- Access to information, documents, and database records.
- Operations that can be performed on the accessible information.
- Access to API and Web services.
- The data that will be returned to the client by a REST service.

4. What are the key features of the latest release of Access Management 11gR2 Patch Set 2 (11.1.2.2.0)?

- A unified Administration Console for Access Manager, Identity Federation, Security Token Service, Mobile and Social, and Access Portal configurations.
- Automation tools for installation and patching
- The new Access Portal Service
- Identity Federation Identity Provider integrated into the Access Management Suite
- Access Manager

- Delegated Administration
- Granular Idle Timeout
- Policy Re-ordering
- Dynamic Authentication / Advanced Rules
- Enhanced 10g / 11g Co-existence approach
- Cookie Based Session Management
- Improved Multi-Data Center Deployment
- IPv6 Support

- Mobile and Social
  - Server-side Mobile SSO
  - JWT/OAM Token Exchange
  - Mobile Client based federation
  - Built-in app registration for mobile clients
- OAuth 2.0 Service
  - 3-legged and 2-legged OAuth
- API Gateway
  - Enhanced Test to Production Deployment Promotion Support
  - Configuration Diff and Merge Support
  - Embedded OAuth token store and KPS backing store
  - Monitoring and Logging Enhancements
- Entitlement Server
  - Fine Grained Authorization for "WebCenter Content" managed Documents and Records, and Management Operations
  - Enhanced HA and Disaster Recovery Support
  - Performance enhancements

5. What are the key features of Access Management 11gR2 Patch Set 1 (11.1.2.1)?

- Heterogeneity - Websphere Application Server 7.0 support for all Access Management products
- Authentication and SSO
  - 11g WebGate for IBM HTTP Server 7.0
  - Enhanced Security and user experience
  - Improved OpenSSO/Sun Access Manager (SAM) migration tools
  - Multi-data Center support enhancements
- Mobile and Social
  - SDK support for Android
  - Additional social providers such as Windows Live
  - Mobile offline authentication
  - Social identity to local account linking
- Enterprise Single Sign-On
  - OPAM integration
- Adaptive Access Manager
  - Simplified user experience with single page login flow, no virtual pad
- Entitlements Server
  - Improved user experience for very large deployments
  - New out of the box 3rd party application server certifications
  - Oracle Fusion Middleware integration
  - .NET and Sharepoint 2010 integration
  - Policy Simulation
  - Multiple ID Store support
- API Gateway
  - OAUTH 2.0 support
  - Improved REST and JSON Support
  - Improved API Key Management
  - New unified UI console
  - New deployment / clustering model
  - Access Manager 11gR2 Access SDK based integration
  - Integration with Oracle Business Transaction Monitor
  - Parameterized Policies

4. I am developing a custom integration that needs to interact with Oracle Access Management. Where can I find available sample code?

All sample code is published on *the Sample Code for Developers and Admin* site located at

http://www.oracle.com/technetwork/indexes/samplecode/id-mgmt-1884959.html

Integration Questions

1. Where do I find information regarding Identity and Management integration?

The Integration Overview for Identity and Access Management products is the best place to start. It can be found at

http://docs.oracle.com/cd/E37115_01/index_prod.htm

2. Where do I find guides for integrating Access Management products with other Oracle Products (such as Oracle E-Business Suite, PeopleSoft, JD Edwards, and Siebel)?

The documentation on how to integrate these Oracle products with Oracle Access Management (specifically Access Manager) can be found in the documentation sets for the appropriate product or as a knowledge base article on Oracle Support.

Oracle Access Management Access Manager (Access Manager)

This section contains frequently asked questions related to Access Manager.

General Questions

1. What is Oracle Access Manager?

Oracle Access Manager (Access Manager) is the foundation of the new Oracle Access Management platform; it provides the core functionality for Web Single Sign-on (SSO), authentication, authorization, centralized policy administration and agent management, real-time session management, and auditing. Built as a 100% Java solution, Access Manager is extremely scalable allowing it to handle Internet scale deployments. It also works with existing heterogeneous environments with agents certified for hundreds of web servers and application servers. Access Manager provides rich functionality, scalability and high availability thereby increasing security, improving user experience and productivity, and enhancing compliance while reducing total cost of ownership.

2. What are the key features of Access Manager 11gR2 Patch Set 2 (11.1.2.2)?

- Delegated Administration
- Granular Idle Timeout
- Dynamic Authentication / Advanced Rules
- Policy Re-ordering
- Enhanced 10g / 11g Co-existence approach
- Cookie Based Session Management
- Improved Multi-Data Center Deployment
- IPv6 Support

3. What are the key new features of Access Manager 11gR2 Patch Set 1 (11.1.2.1)?

- Heterogeneity
  - WebSphere Application Server 7.0 support
  - 11g WebGate for IBM HTTP Server
- Enhanced security and user experience including post data preservation and language drop-down selection on the login page
- Improved OpenSSO/SAM migration tools
- Excel based assessment report
- OpenSSO 8.0 and SAM 7.1 Incremental mode migration
- Multi-data Center support enhancement – read-only Data Center enforcement

4. What are the key features of Access Manager 11gR2 (11.1.2.0)?

- LDAP Server Filters in Identity Conditions
- Attribute Class Authorization Conditions - Session, request or user attribute
- Complex Authorization Expressions
- Detached Credential Collection
- Dynamic Multi-Factor / Multi-Step Authentication
- Restful Policy Administration Interfaces
- Password Management
- Server side co-existence with OAM 10g, OpenSSO 8 and SAM 7.1
- Support for Multi-Data Center Deployment
- Third party Integrations (including Microsoft Sharepoint, RSA Authentication Manager 7.1, JBoss 5.0)

5. What is the Detached Credential Collector in Access Manager 11gR2?

The Detached Credential Collector (DCC) is essentially an 11g WebGate that has been extended to provide credential collection capability. The DCC can be used to replace the

login page on the server (also known as an Embedded Credential Collector or ECC).

6. What advantages does the DCC offer as compared to the ECC?

The DCC offers a number of benefits from a security and a flexibility point of view. Since the DCC is completely decoupled from the Access Manager server, it can be deployed anywhere in the DMZ. It also provides added security because all unauthenticated end user login requests get terminated at the DCC in the DMZ so the server is isolated from unauthenticated network traffic.

7. We are considering a high-availability deployment of Access Manager 11gR2. What are our options?

Access Manager 11gR2 is built as a 100% Java solution and is designed for extreme scalability and high availability. Customers looking for a high-availability deployment should consider:

- Deployment in WebLogic clusters for scaling horizontally within a single data center.
- Multi-data Center deployments for scaling across data centers. They can be configured in Active – Active, Active-Passive or Active – Hot Standby modes.

8. Access Manager 11g WebGates are supported on Oracle HTTP Server 11g and IBM HTTP Server 7.0 but I use Apache Web Servers. What do I do if I want to use Access Manager 11g?

Access Manager 11g servers are capable of communicating with Oracle Access Manager 10g WebGates. Oracle Access Manager 10g WebGates have a broad set of certifications for web servers including various versions of Apache, Domino, Microsoft IIS, and many more. Refer to the certification matrix for a list of supported configurations:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

9. Does Access Manager 11g support x-509 authentication?

Access Manager 11g supports x-509 authentication as long as the certificate is provided with the HTTP request.

Certification Questions

1. Is there a direct link to the certification matrix for 10g WebGates that are supported against Access Manager 11g Server?

The certification matrix for 10g WebGates can be found under the WebGates tab at

http://www.oracle.com/technetwork/middleware/downloads/oracle-accessmgr-10gr3-certmatrix-132000.xls.

2. I don't see the WebGate configuration I want listed on the certification matrix. How do I request a new WebGate?

Log a Service Request with Oracle Support and indicate that it is a request for certification to support a new Access Manager WebGate.

Migrations Questions

1. I am currently running Oracle Access Manager 10gR3. How do I migrate to Access Manager 11gR2 (11.1.2.x)?

Access Manager 11gR2 provides assessment / migration tools, server side co-existence and agent backward compatibility to help customers with 10g migration projects. For details, refer to the Migration Best Practices for Oracle Access Manager 10gR3 Deployments Whitepaper available at

http://www.oracle.com/technetwork/middleware/id-mgmt/index-090417.html

Additionally, the *Upgrade and Migration Guide for Oracle Identity and Access Management*, published as part of the 11.1.2.x product documentation set, contains information.

2. I have a large Oracle Access Manager 10gR3 deployment with thousands of WebGates. Do I need to upgrade them all to migrate to the new Access Manager 11gR2 platform?

No. Access Manager 11gR2 provides agent backward compatibility that allows 10gR3 customers to continue using their existing 10gR3 (10.1.4.3) WebGates. A protocol compatibility framework allows the Access Manager server to communicate with 10gR3 WebGates the same way it can communicate with the new 11g WebGates. Therefore, Access Manager 10gR3 customers with large deployments can focus on upgrading their server infrastructure first and adopt a more phased approach for replacing their existing 10gR3 WebGates with new 11g WebGates over time.

3. I have a large Oracle Access Manager 10gR3 deployment with thousands of applications. Do I need to migrate them all to the new 11gR2 platform at once?

No. Access Manager 11gR2 provides server side co-existence where both the Oracle Access Manager 10gR3 and Access Manager 11gR2 servers can be live in production at the same time protecting different sets of applications. End users will continue having a seamless single sign-on experience as they navigate between applications protected by the two servers. This capability can be leveraged by customers with large deployments to perform the server migration in a phased manner over a period of time without impacting end users.

4. I am a Sun Access Manager 7.1 or OpenSSO 8.0 customer. How to I migrate to Access Manager 11gR2?

Access Manager 11gR2 provides assessment / migration tools, server side co-existence and agent backward compatibility to help customers with 10g migration projects.

For more details, please refer to the Migration Best Practices for OpenSSO 8 and Sun Access Manager 7.1 deployments Whitepaper available at

http://www.oracle.com/technetwork/middleware/id-mgmt/index-090417.html

Also the *Upgrade and Migration Guide for Oracle Identity and Access Management* published as part of the 11.1.2.x product documentation set.

5. I have a large Sun Access Manager 7.1 or OpenSSO 8.0 deployment with thousands of Policy Agents. Do I need to upgrade them all to migrate to the new Access Manager 11gR2 platform?

No. Access Manager 11gR2 provides agent backward compatibility that allows Sun Access Manager 7.1 or OpenSSO 8.0 customers to continue using their existing Policy Agents (versions 2.2 and 3.0). A protocol compatibility framework allows the Access Manager server to communicate with Policy Agents the same way it can communicate with the new 11g WebGates. Therefore, Sun Access Manager 7.1 and OpenSSO 8.0 customers with large deployments can focus on upgrading their server infrastructure first and adopt a more phased approach for replacing their existing Policy Agents with new 11g WebGates over time.

6. I have a large Sun Access Manager 7.1 or Sun Access Manager 7.1 deployment with thousands of applications. Do I need to migrate them all to the new Access Manager 11gR2 platform at once?

No. Access Manager 11gR2 provides server side co-existence where both the OpenSSO 8.0 (or Sun Access Manager 7.1) and Access Manager 11gR2 servers can be live in production at the same time protecting different sets of applications. End users will continue having a seamless single sign-on experience as they navigate between applications protected by the two servers. This capability can be leveraged by customers with large deployments to perform the server migration in a phased manner over a period of time without impacting end users.

7. I am an Oracle Single Sign-on customer. How do I migrate to Access Manager 11gR2?

Access Manager 11gR2 offers the upgrade path and server side co-existence. The process is described in the Upgrade Guide that can be found at

http://docs.oracle.com/cd/E27559_01/index.htm

Oracle Access Management Mobile and Social (Mobile and Social)

This section contains frequently asked questions related to Mobile and Social.

General Questions

1. What is Oracle Access Management Mobile and Social?

Oracle Access Management Mobile and Social (Mobile and Social) is a solution that securely extends existing Access and Directory solutions to mobile devices using feature-rich platform specific client side SDKs and industry standards including REST, JSON, and OAuth. Social network identities like Facebook and Google can optionally be used to log in and gain access to resources protected by Oracle Access Manager. Mobile and Social is tightly integrated with Oracle Access Manager and Oracle Adaptive Access Manager, and installs preconfigured with these components as part of the Access Management installation.

2. What versions of Access Manager can be used with Mobile and Social?

Mobile and Social supports Oracle Access Manager 10gR3 (Server and WebGates), Access Manager 11gR1 (11.1.1.5+) and Access Manager 11gR2 (11.1.2.x). Please refer to the certification matrix for more details:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

Mobile Single Sign-On is supported for native mobile applications and application access via the mobile browser.

3. What additional capabilities does Mobile and Social offer when used with Oracle Adaptive Access Manager?

When Mobile and Social is combined with Oracle Adaptive Access Manager 11gR2 (11.1.2.x), the following additional features are available:

- Advanced device fingerprinting and historical tracking
- Advanced device registration
- Policy support to address lost and stolen devices
- GPS and Wifi location awareness
- Risk-based Knowledge Based Authentication (KBA) and email /SMS One-Time Password (OTP)
- Transactional risk analysis

4. I am upgrading to Access Manager 11gR2 (11.1.2.x). What do I need to do to add Mobile and Social?

When Access Manager 11gR2 (11.1.2.x) is installed, Mobile and Social features are also installed although not initially active. Turn on the Mobile and Social feature set by accessing the Available Services page from the Oracle Access Management Administration Console.

5. Which Social identity providers can be used out of the box?

Mobile and Social supports Google, Facebook, Yahoo, Twitter and LinkedIn out of the box. Mobile and Social integrates with these identity providers using OAuth and OpenID standards. Additional providers can be added via Mobile and Social's Social Identity API. Refer to the certification matrix for details:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

Contact Oracle Consulting Services or your implementation partner for more information on additional providers.

6. Does Mobile and Social work with Oracle API Gateway?

Mobile and Social and Oracle API Gateway (OAG) are integrated to provide an end-to-end solution for using Secure API for mobile and other types of applications. OAG:

- Provides API Management, threat protection, client side throttling, transport and message / content level security, OAUTH capabilities, fine grained authorization and data redaction (through integration with Oracle Entitlements Server), and many other things for REST, SOAP, JMS and other type of API and web services exposed to mobile applications (and other types of clients).
- Provides the same level of protection for the Oracle Access Management Mobile / Social REST based endpoints.
- Acts as a WebGate and enforcement point using either Oracle Access Management Mobile / Social JWT tokens or OAM tokens, and extends Oracle's Web Access Management / SSO solutions to web services.
- Provides protocol and security token translation. For example, internal SOAP based web services leveraging SAML for authentication and identity propagation can be exposed to mobile applications as secure REST API based on OAM/JWT Tokens.

7. What are Mobile and Social User Profile Services, and for which directories can Mobile and Social provide User Profile support?

User Profile services allows Mobile and Social to offer user and administrator access to configured directory services. User Profile services can be used for Corporate or Community White Pages, User Self-Registration and Self-Service, and Directory Administration tools. Additional functionality includes the ability to search, view, create, update and delete Users, Groups and Relationships (such as a user's manager)

User Profile services provide REST interfaces to all Oracle LDAP directories, Including Oracle Unified Directory (OUD), Oracle Directory Server Enterprise Edition (ODSEE), Oracle Internet Directory (OID), and the WebLogic server embedded LDAP, and also supports other industry standard directories such as Microsoft Active Directory, Novell eDirectory and Open LDAP. Refer to the certification matrix for details:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

8. What client SDKs are available for Mobile and Social?

Mobile and Social 11gR2 (11.1.2.2.0) offers a Mobile and Social SDK for JAVA, iOS, and Android.

9. My mobile platform does not have an SDK. Can I still use Mobile and Social?

All interactions from devices and applications and the Mobile and Social server take place with REST calls made over the HTTP/HTTPS protocol. These RESTful interfaces are incorporated into all Mobile and Social Client SDKs (including iOS, JAVA and Android), and serve as the foundation for those SDKs. For those platforms and scenarios supported by an SDK, the SDK simplifies using Mobile and Social, and standardizes client-side functions such as SSO and credential storage. If your solution requires support on a device that does not have an SDK (such as a BlackBerry device), or your requirements are not met by the SDK, the REST API is available.

Oracle Access Management Access Portal (Access Portal)

This section contains frequently asked questions related to Access Portal.

General Questions

1. What is Oracle Access Management Access Portal (Access Portal)?

The Access Portal service provides a cross-platform single sign-on service for web-based applications including SaaS applications, Oracle Access Management protected resources and business partner applications.

2. How is Single Sign-on achieved?

Single Sign-On is achieved through a variety of methods, including Oracle Access Management tokens (SSO to Oracle Access Management protected resources), Identity Federation (SSO to federation-enabled SaaS and business partner applications) and Form-Fill (SSO to non-federation enabled web applications - including SaaS).

3. How do you integrate Access Portal into an existing or a newly developed user portal?

Access Portal can be integrated into an existing or newly developed user portal using the available RESTful interfaces.

Oracle Adaptive Access Manager

This section contains frequently asked questions related to Oracle Adaptive Access Manager (OAAM).

General Questions

1. What is Oracle Adaptive Access Manager?

Oracle Adaptive Access Manager (OAAM) is utilized to prevent web application access fraud and misuse. OAAM provides multiple layers of security such as device fingerprinting, location intelligence, behavioral profiling, real-time risk analysis and risk-based identity verification, interdiction and alerting. The OAAM security layers combat modern online threats including compromised authentication credentials, session hijacking and insider fraud.

2. What are the new features of OAAM 11gR2 (11.1.2.x)?

OAAM 11gR2 provides improved mobile access security, enhanced multi-channel fraud detection capabilities, layered security for cloud service providers and new forensic tools to speed fraud investigations. Providing centralized, layered security and risk-based authentication capabilities for both standard web and mobile access is a new feature. The ability to evaluate access and transactional risk from non-web sources will help customers to more holistically secure their enterprise.

Security is still the main barrier to cloud service adoption in the enterprise space so the ability for service providers to provide added layers of protection is key to business growth. When a human fraud investigator is required to evaluate an alert, OAAM helps them to determine what the situation is and locate the related fraud quickly and painlessly.

3. How can OAAM save my company money?

OAAM can help reduce negative impacts to a company's bottom line by preventing fraud and misuse of sensitive applications and the data they contain. Brand damage resulting from a publicized security breach can be very expensive in both the short and long term for an enterprise. Additionally, prevention of fraud can directly save large sums of money for an enterprise. By verifying user identities via multiple security layers and evaluating the risk of transactions in real-time, OAAM pays for itself in an average of one year. For more ROI details, read the IDC ROI study.

4. How can OAAM improve self-service password management flows?

Businesses primarily develop self-service flows to reduce costly help desk calls so the flows must be highly secure and usable. One of the most critical flows is the *Forgot Password?* reset. If the flow is not completed in a secure manner, this can introduce a weak link in the perimeter security. As well, if the reset flow is not easy to follow, end users will call the help desk, defeating the whole purpose of a self-service flow. OAAM layered security secures flows with device fingerprinting, behavioral profiling, risk analysis and risk-based authentication. If challenge questions are utilized as the alternate authentication mechanism in the *Forgot Password?* Flow, OAAM can increase user success by allowing variability in the answers submitted; OAAM can even negotiate typos, abbreviations and date format variances to increase usability. The unique combination of layered security and the OAAM Knowledge Based Authentication (KBA) Answer Logic can help your business ensure that both help desk calls and fraud will be reduced.

5. What impact does KBA have on user experience?

Large consumer facing OAAM deployments with multiple millions of users have reported that their customer support call volumes increased by approximately .2% during roll out and decreased shortly thereafter. When all answer logic was enabled and set to "low" approximately 7% of KBA challenges resulted in a call to support for reset with answer logic turned up to high this number reduces by roughly half. Large OAAM deployments actively using the CSR phone challenge feature have been very satisfied with the results

and have reported that valid users are consistently able to answer their questions over the phone 95% of the time.

6. What is OAAM auto-learning?

Auto-learning is a set of functions in OAAM that profiles behavior. The behavior of users, devices, locations and transactions themselves are recorded and used to evaluate current behavior. For example, OAAM can profile a user based on login time. If John logs in between 8am - 10am 87% of the time then the risk level is elevated if he is attempting to login at 2am. In other words he is outside of his normal login time profile. OAAM evaluates "learns" in real-time the combination of multiple data points and how they relate to one another. This allows for the risk evaluation to automatically adjust when a valid user changes their behaviors over time.

7. Do customers need to engage with Oracle to implement new security risk policies?

No. OAAM provides a business used friendly GUI to configure risk policies using generic rule conditions that may be configured to accomplish any foreseeable use case. New policies can easily be tested against production data to assess the effect.

8. How does OAAM integrate with applications to perform transactional risk analysis?

OAAM provides Java, .Net and SOAP APIs for in-line application integration. OAAM also provides the Java Message Service Queue asynchronous and batch based options as well for out of line use cases.

9. For what languages is OAAM globalized?

OAAM is globalized to the Oracle standard set of languages for which all products are required to support. The end user facing screens are translated to the STD_RUNTIME set of 26 languages and the OAAM administration console is translated to the STD_ADMIN scope of 9 languages. The up to date language scope can be found here.

Oracle Enterprise Single Sign-On Suite Plus

This section contains frequently asked questions related to Oracle Enterprise Single Sign-On Suite Plus.

General Questions

1. What is Oracle Enterprise Single Sign-On Suite Plus?

Oracle Enterprise Single Sign-on Suite Plus (eSSO) allows users to log in to enterprise applications using a single password for any password-protected application on the desktop, network or Internet. It offers a highly scalable enterprise single sign-on infrastructure, providing features such as single sign-on, client-side Windows password reset, centralized user provisioning, support for kiosk environments, strong authentication, and comprehensive auditing. With eSSO, users can truly authenticate once and have access to all the applications they access on a day-to-day basis.

2. What are the key features of Oracle Enterprise Single Sign-On Suite Plus 11gR2 (11.1.1.2.x)?

- User to User Account Delegation allows users to securely pass their credentials from one user to another.
- Seamless integration with Oracle Access Manager provides organizations the ability to implement a single SSO session no matter what type of application is being accessed.
- eSSO – UAM now supports Windows 7 for Smart Card, Proximity Card, Biometric and Knowledge Based Authentication
- Re-engineered support for Firefox browsers to take advantage of Mozilla's rapid release schedule.

3. Is Oracle Enterprise Single Sign-On Suite Plus deployable using software distribution tools?

Yes, eSSO is deployable using any software distribution tool that can deploy a standard MSI file. The eSSO Administrative Console provides an easy way to customize the standard Oracle eSSO MSI and customize a deployment package that is ready to be distributed with Microsoft's SMS or nearly any other distribution tool (including Novadigm, Tivoli, Marimba or even just a Web download).

4. Is Oracle Enterprise Single Sign-On Suite Plus available on other platforms such as iOS and Android?

Yes, eSSO customers can use the Access Portal service to provide cross platform single sign-on for web based applications. See the FAQ regarding Access Portal for details.

5. Can I centrally control Oracle Enterprise Single Sign-On Suite Plus administrative settings?

Yes. eSSO administrative settings are controlled using the Administrative Console's easy-to-use GUI. eSSO leverages your existing infrastructure as the central repository. eSSO supports various directories (including Oracle Unified Directory (OUD), Oracle Directory Server Enterprise Edition (ODSEE), Oracle Internet Directory (OID), Microsoft Active Directory & ADAM) or a database (Oracle, DB2, SQL) as a central repository for user and administrative settings. Simply store the application definitions, password policies and eSSO configuration settings in the eSSO configuration objects on the directory and each Oracle eSSO client will pull down the newest configuration data each time it starts up.

6. Can the administrator control which applications are accessed via single sign-on and which are not?

Yes. This is configurable globally, by role/group, or user. As such, we can support flat directories or detailed hierarchical directories.

7. Is it possible to deactivate a user account for some or all of the applications?

Yes. This can be done via the eSSO-Provisioning Gateway.
8. Can you limit (by user, group and/or application) the ability of the user to see (have revealed to them) their own passwords?

Yes. The Reveal button can be toggled. All eSSO settings can be assigned on a global, role/group or user basis.

9. Can users switch from one workstation to another transparently?

Yes. eSSO-LM grants users single sign-on access from any workstation that has the eSSO-LM client software.

10. How do you configure Oracle Enterprise Single Sign-On Suite Plus to respond to an application?

Through the Administration Console, an administrator defines an application template that contains the exe name, the windows title, and the Control ID field of the application. The eSSO agent then uses this template to monitor each application launched on the workstation. When an application detects a configured application it responds on behalf of the user. There is no need for backend server integration between eSSO and the applications being enabled.

11. Is it possible to have different accounts to the same application for one user? If so, describe the behavior.

Yes. If a user has two accounts for one application, eSSO-LM will provide the user with a "Logon Chooser" window which enables the user to select the login account.

12. How does an Oracle Enterprise Single Sign-On Suite Plus architecture provide failover?

eSSO typically leverages a corporate directory and therefore benefits from the directory's fault tolerance and redundancy features.

13. Does Oracle Enterprise Single Sign-On Suite Plus support Strong Authentication?

eSSO has a module called Universal Authentication Manager that provides smart card, biometric and proximity card authentication. eSSO can also leverage RSA Secure ID tokens as well as achieve native certificate based smart card authentication with National ID cards, CAC card, PIV Cards and corporate issued smart cards.

14. Does Oracle Enterprise Single Sign-On Suite Plus support resetting the Windows Password?

Yes. The Oracle Password Reset (eSSO-PR) enables end users to reset their primary authentication (Windows) password from a locked workstation based on a challenge-response process. When Oracle eSSO-PR is installed, users enroll by answering a series of confidential questions. If a user forgets the Windows password, Oracle eSSO-PR prompts for an answer to the questions. An identity validation process compares the entered answers with the defined answers; it factors in human errors in typing and memory recall (confidence based authentication). If the user successfully answers a sufficient number of questions, Oracle eSSO-PR enables them to automatically reset their Windows password - with no call to the help desk. All questions are customizable and configurable.

15. How does Oracle Enterprise Single Sign-On Suite Plus store data on my directory server(s)? Do you modify the base schema?

Product development has collaborated with leading suppliers of enterprise directories in designing our approach to supporting Directory Servers. eSSO uses an effective class schema extension which leaves your base schema intact - as delivered by your directory vendor - and creates a self-contained configuration object using our own object classes. By comparison, some companies make a base schema extension that modifies your base schema (specifically the user object) and appends SSO data to it, causing problems with network traffic during directory upgrades and directory replication - as the user object is always replicated.

16. How does Oracle Enterprise Single Sign-On Suite Plus encrypt and protect my logon credentials?

eSSO creates a unique primary symmetric key for each user; this key is used when encrypting the user's credentials. End-to-end encryption is provided between the eSSO agent and the Directory using the selected encryption algorithm. eSSO's default encryption algorithm is the MS CAPI-provided AES. Credentials are stored encrypted on the PC,

in transit and in the Directory. Credentials are not stored unencrypted in memory.

17. Is Oracle Enterprise Single Sign-On Suite Plus FIPS 140-2 compliant?

Yes, eSSO uses the MS CAPI-based 256 Bit AES which is certified to meet FIPS 140-2 requirements for United States Government customers.

18. How does Oracle Enterprise Single Sign-On Suite Plus prevent the administrator from learning users' passwords?

Administrators do not know the users' passwords as all passwords are stored in an encrypted format. Further, to avoid attacks by rogue administrators, eSSO can be configured to require a secondary form of user authentication (a passphrase) before enabling SSO from a reset password.

19. How does Oracle Enterprise Single Sign-On Suite Plus prevent an administrator from resetting the Windows password and impersonating a user to access the user's stored credentials?

To prevent the administrator from impersonating a user, the authenticator is configured to prompt the user for a passphrase during enrollment. The user must provide the passphrase whenever eSSO detects that the Windows Password has been reset. If the administrator resets the Windows password, in order to gain access to the stored credentials, the administrator would need to know the user's secret passphrase. The passphrase also protects your credentials in the event that your PC/laptop is lost or stolen.

Oracle Access Management Identity Federation (Identity Federation)

This section contains frequently asked questions related to Identity Federation.

General Questions

1. What is Identity Federation?

Identity Federation is a complete, enterprise-level and carrier-grade solution for exchanging secure identity information between partners. It significantly reduces the need to create and manage unnecessary identities in an enterprise directory and lowers the ongoing costs of partner integrations through its support of industry federation standards. Identity Federation protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers and applications. With Identity Federation, organizations can do more business online by allowing their business partners secure access to protected applications.

2. What are the benefits of Oracle Access Management Identity Federation 11gR2 (11.1.2.x)?

The Identity Federation service is a core component of Oracle's industry leading identity and access management platform. The 11*g* R2PS2 release moves towards a fully converged federation service architecture within Oracle Access Management, enabling several common business scenarios to seamlessly work out of the box. These include built-in support to leverage any Access Manager Authentication Scheme for User authentication at the Identity Provider, providing built-in support for risk assurance and fraud detection in a federated scenario at the Service Provider, built-in authentication, authorization and attribute passing with Oracle Access Management across federated sessions and a unified administration, installation and configuration experience.

3. What are the key features of OAM Identity Federation 11gR2 (11.1.1.2.x)?

- Support for all major industry protocols
- Social Identity Support and social login registration
- Fully converged service within OAM for both Identity Provider and Service Provider functionality
- Support for all OAM Authentication Schemes for IDP authentication
- Built-in support for risk and fraud awareness in a federated session
- Support for multiple identity stores for authentication and attribute exchange
- Identity Provider Discovery
- Identity Provider Proxy
- Support for industry standard attribute sharing profiles
- Support for attribute profiles for both IDP and SP
- Quick and easy federation partnership setup across all protocols
- Proven Internet Level Availability and Scalability
- Provisioning Plug-in Framework
- Unified administration, installation and deployment within Oracle Access Management

4. What protocols are supported by Oracle Access Management Identity Federation 11gR2 (11.1.1.2.x)?

- SAML 2.0
- SAML 1.1
- OpenID 2.0
- FICAM (Federal Identity, Credential, And Access Management):
  - ICAM SAML 2.0 Web Browser SSO Profile - (Level of Assurance 1, 2, non-crypto 3).
  - ICAM OpenID 2.0 Profile (Level of Assurance 1)

5. Does Oracle Access Management Identity Federation 11gR2 (11.1.1.2.x) support attribute sharing?

Yes, it supports industry standard attribute sharing:

- SAML Attribute Sharing Profile - SAML provides an Attribute Query/Response protocol for retrieving a principal's attributes.
- OpenID Attribute Exchange (AX) - AX is an OpenID 2.0 extension
- ICAM BAE (Backend Attribute Exchange) Direct Attribute Exchange
- ICAM BAE Broker Attribute Exchange - via an integration with the Oracle API Gateway

6. What is the OAuth2.0?

OAuth 2.0 is a standards compliant OAuth 2.0 authorization service implementation that supports both 3-legged and 2-legged OAuth flows and the following roles defined by OAuth:

- Resource Server: hosts the protected resources, capable of accepting and responding to resource requests using access tokens.
- Client**:** makes protected resource requests on behalf of the resource owner and with its authorization. The term client is not specific to a particular entity; for example, the client could be an application that executes on a server or on a mobile device.
- Authorization Server**:** issues access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

.

7. What is the benefit of using the OAuth2.0 protocol for secure access?

In the traditional client-server authentication model, the client accesses a protected resource on the server by authenticating with the server using the resource owner's credentials. In order to provide third-party applications access to protected resources, the resource owner shares their credentials with the third-party. This creates the following problems and limitations:

- Third-party applications are required to store the resource owner's credentials for future use - typically a password in clear-text.
- Servers are required to support password authentication despite the security weaknesses created by passwords.
- Third-party applications gain overly broad access to the resource owner's protected resources leaving them without the ability to restrict duration or access to a limited subset of resources.
- Resource owners cannot revoke access to an individual third party without revoking access to all third parties and must do so by changing their password.

The OAuth 2.0 protocol addresses these issues by introducing an authorization layer and separating the role of the client from that of the resource owner. In OAuth 2.0, the client requests access to resources controlled by the resource owner and hosted by the resource server and is issued a different set of credentials than those of the resource owner. Instead of using the resource owner's credentials to access protected resources, the client obtains an access token - a string denoting a specific scope, duration, and other access attributes. An authorization server with the approval of the resource owner issues access tokens to third-party clients. The client uses the access token to access the protected resources hosted by the resource server.

8. What is the benefit of using the Oracle Access Manager OAuth 2.0 Service?

The OAuth 2.0 Service provides a fully standards compliant OAuth 2.0 authorization Server with support for both 3-legged and 2-legged OAuth flows and enables the OAuth 2.0 Client and the OAuth 2.0 Resource Server roles. It uniquely provides several compelling differentiations and innovations for mobile OAuth 2.0 clients (such as native applications on mobile devices) specifically for extranet access in enterprise scenarios. These include built-in support for mobile application registration and device identification during the OAM OAuth 2.0 mobile flow ensuring trusted access from mobile devices and built-in server side single sign on for mobile OAuth clients. It is ideally suited for enterprise scenarios that may require higher levels of security during an OAuth flow and would benefit from built-in OAM integrations provided by the OAM OAuth 2.0 service.

9. What is the difference between OAM Classic OAuth and OAM Mobile OAuth?

OAM Classic OAuth provides 3-legged and 2-legged OAuth flows for non mobile clients while OAM Mobile OAuth enables those flows for mobile clients. Mobile clients are categorized as native applications on mobile devices.

10. What is the significance of securing enterprise mobile clients using OAuth?

Several OAuth clients are consumer applications that cannot keep the client secret confidential (application password or private key). These OAuth clients are called public clients or non-confidential clients. Mobile Client applications (native applications on mobile devices) are also categorized as public clients because when a native

application is first downloaded from an app store to a device it has the client credentials that uniquely identify the client application baked into the application. Since all users that download the native application have access to the binary, a malicious user could easily decompile the client credentials out of the binary and insert their own credentials. During an OAuth flow, a major vulnerability is apparent when the access code gets exchanged for the access token as there is no secure means of really identifying who is actually receiving and using the access token. Hence, providing a mechanism to secure the mobile application on the device in order to ensure trusted access is a key requirement specifically for enterprise mobile applications that routinely require access to sensitive data.

11. What are some key features provided by the OAM OAuth service to secure enterprise mobile access?

The OAM OAuth 2.0 Service provides built-in support for a mechanism that allows mobile applications to be first registered with OAM to use OAuth Access Services. The mobile application always submits this registration based client token as an input parameter for accessing OAM OAuth 2.0 Service end points. Furthermore, the OAM OAuth 2.0 service also allows built-in coupling of device identification with mobile application registration where mobile devices and applications are checked against fraud and security using a built-in integration with Oracle Adaptive Access Manager (OAAM). In addition, the mobile OAuth 2.0 flows in the OAM OAuth 2.0 provides the following features for secure enterprise mobile access:

- Native support for APNS or GCM for secure OAuth token delivery
- Secure Server-side Mobile SSO (no requirement on SDK) for all mobile OAM OAuth 2.0 clients

12. What are some key differentiations provided by the OAM OAuth service as a built-in service within Oracle Access Manager?

- Built-in integration with OAM during resource owner authentication and consent allowing:
  - Leverage OAM authentication scheme(s)
  - Fraud Detection & Strong Authentication
  - Single Sign On and Session Management
- OAM Resource Protection
  - Allow protecting OAM webgate resources with OAuth tokens.
- Common OAM configuration, deployment and infrastructure
- Multi-Tenancy support for Cloud deployments
- Extensions Support for OAuth Assertion specifications for SAML bearer & JWT tokens

13. What are some key considerations for choosing between OAM OAuth and the OAuth service in Oracle Application Gateway?

Both products support 3-legged and 2-legged OAuth flows but they are designed to support different use cases. Customers that are looking for an access management platform or would like to leverage their existing investment in Oracle Access Management but also require OAuth2.0 functionality are ideally suited to leverage the OAM OAuth 2.0 Service while those customers that are looking for an API security solution which can coexist with Oracle or other Access Management platforms may leverage Oracle Application Gateway (OAG) OAuth. Use the OAM OAuth 2.0 Service to leverage out of the box OAM integrations, provide secure mobile client access to APIs and provide higher levels of security that are required during enterprise OAuth flows. Use the OAG OAuth 2.0 Service for enterprise access to cloud based APIs acting as a Cloud API Gateway and to provide support for non confidential clients.

Oracle Access Management Security Token Service (Security Token Service)

This section contains frequently asked questions related to the Security Token Service (STS).

General Questions

1. What is the Oracle Security Token Service?

Security Token Service (STS) is the next generation token service from Oracle, designed to facilitate Identity propagation across web services.

2. What are the primary usage scenarios of the Security Token Service?

Web-to-Web Service Identity Propagation

In this scenario, a user's identity information needs to be propagated from a web application to a web service provider. The web service provider could reside in the same security domain as the web application or in a different security domain altogether.

Web Service-to-Web Service Token Exchange

In this scenario, a user is authenticated into a domain using a certain type of credentials, for example username/password, X.509 certificate or Kerberos. However, in order for the user to access or communicate with a web service provider, a SAML token is required. In cases such as this, Oracle STS can facilitate token exchange from one standard token format to another (e.g., SAML 1.x or SAML 2.0). Once again, the web service provider could reside in the same or different security domain as the web service consumer.

3. What is the role of the WS-Trust protocol relative to the Security Token Service?

WS-Trust is the protocol used for communicating with an Oracle STS server. WS-Trust defines:

- The concept of a "security token service"
- The message formats used to request and issue security tokens
- The mechanisms for key exchange

4. What features are supported by the WS-Trust provider in Oracle Web Services Manager?

- Requesting an issue token from the Security Token Service
- Verifying and processing the Security Token Service-issued token on the service side and generating responses
- Configuring the client or service policy to request tokens from a specific Security Token Service instance

5. How does the OWSM WS-Trust Provider interact with Security Token Service?

When OWSM is leveraged as a WS-Trust client for Oracle STS, the OWSM WS-Trust provider is used to send WS-Trust requests to the STS. Once OWSM receives a WS-Trust response from the STS that response is propagated to the Web Service. OWSM WS-Trust client supports the following primary use cases with STS:

1) Token exchange/conversion

   OWSM Trust client enables users to exchange basic tokens (requestor tokens) for SAML Tokens (generated by STS)

2) Token exchange on behalf of an entity

   The client has the ability to request a token for itself (subject in the request) or On Behalf Of (OBO) another entity (can be configured in the Issue-Token Client Policy)

6. Which WS-Trust policies are available to Oracle STS?

By default, there are two OWSM policies available to support Security Token Service token exchange with a web service endpoint:

1. STS configuration policies

- oracle/sts_trust_config_client_policy
- oracle/sts_trust_config_service_policy

2. Issue-Token Policies
   - oracle/wss11_sts_issued_saml_hok_with_message_protection_client_policy
   - oracle/wss11_sts_issued_saml_hok_with_message_protection_service_policy
   - oracle/wss11_sts_issued_saml_with_message_protection_client_policy
   - oracle/wss_sts_issued_saml_bearer_token_over_ssl_client_policy*
   - oracle/wss_sts_issued_saml_bearer_token_over_ssl_service_policy*

*Note: One-way SSL needs to be enabled in order to use the saml_bearer issue-token policies.

7. What are the different token types supported by Oracle Security Token Service?

- Username
- Kerberos
- X.509
- SAML 1.1 or 2.0 assertions

8. Does the Security Token Service support Access Manager tokens as an inbound token?

Yes, STS supports Access Manager 11g session token as an "On Behalf Of" (OBO) token for the end user and can translate this as a SAML or UNT outbound token.

Oracle Web Services Manager

This section contains frequently asked questions related to Oracle Web Services Manager (OWSM).

General Questions

1. What is Oracle Web Services Manager?

Oracle Web Services Manager (OWSM) provides last-mile SOA and REST API security. It is a standards-compliant solution delivered as part of Oracle SOA Suite and the Oracle Access Management Suite that allows you to:

- Centrally define and store declarative security policies for the API's and web services making up an organizations web services & SOA infrastructure
- Locally enforce security and management policies through embedded agents
- Monitor runtime security events such as failed authentication or authorization.

OWSM provides business agility to respond to security threats and security breaches by allowing policy changes to be enforced in real time without the need to interrupt the running business processes.

2. Is Oracle Web Services Manager replaced by the Oracle API Gateway (OAG)?

No. The two complement each other and together provide a layered end-to-end security solution.

OWSM provides last mile / end point security for Oracle Fusion Middleware and Fusion Middleware based applications such as Oracle Fusion Applications. OWSM is the Oracle's strategic solution for providing end point security for REST / SOAP based API's and Web Services and provides embedded agents that run in the same process as the application.

OAG is designed based on a gateway pattern, and deployed in front of an organizations web services and SOA infrastructure, most often in the DMZ.

3. How can I integrate the Oracle API Gateway and Oracle Web Services Manager?

Refer to the following OTN page for details on how to integrate OAG and OWSM:

http://www.oracle.com/technetwork/articles/soa/oeg-owsm-1562313.html

4. How is Oracle API Gateway different from the Oracle Web Services Manager 10g Gateway?

OWSM 10g Gateway and OAG are two separate products. OWSM 10g Gateway was discontinued with the release of Fusion Middleware 11gR1. OAG replaces the earlier OWSM 10g Gateway and is Oracle's strategic API Security/Management and DMZ security solution. OAG also provides a large number of capabilities that were not available in the OWSM 10g Gateway. Refer to the OWSM 10g Gateway to OEG Migration Guide as a starting point for OWSM 10g Gateway to OEG migration.

5. Can I use Access Manager for protecting API's and web services?

Access Manager is a Web Single Sign-on solution and shouldn't be used for protecting REST API's or SOAP based web services. OWSM and OAG are the API and Web Services Security solutions; use one or the other depending on whether you're securing API in the DMZ or within the green zone (corporate network). OAG and OWSM are integrated with Oracle Access Manager for authentication and validation of tokens.

6. How does Identity Propagation between Web and Web Services work when using Access Manager and Oracle Web Services Manager?

Refer to the following blog entry for details on Identity Propagation:

https://blogs.oracle.com/owsm/entry/identity_propagation_across_web_and

Oracle Entitlements Server

This section contains frequently asked questions related to Oracle Entitlements Server.

General Questions

1. What is Oracle Entitlements Server?

Oracle Entitlements Server (OES) is a standards-based, policy-driven security solution that fills the need for granular, flexible, and externalized access control. OES provides authorization policy management and runtime enforcement for sensitive applications, databases, containers (such as Java™ and .NET), portals and content management systems (such as WebCenter and SharePoint), development frameworks, object relational mapping technologies, intermediaries (such as API / XML gateways and ESB's), Web Services, and SOA infrastructure.

Access privileges in OES are defined in a policy by specifying *who can do what, to which set of resources*, *and under what conditions*. The policy can enforce controls on all types of resources, including but not limited to software components (URLs, Java Server Pages, Enterprise JavaBeans, methods, servlets etc.), UI widgets (menus, tabs, portlets, fields, buttons etc.), Business Objects (such as sensitive documents, rich media, images, geospatial information, user profiles, bank accounts, insurance plans, and medical records), REST API's and Web Services among other things.

2. What are the new features of Oracle Enterprise Server 11gR2 (11.1.2.x)?

- Risk and context aware authorization (when used with Oracle Identity and Access Management)
- Support for Policy Simulation
- Support for all data types and functions as defined in the XACML 3.0 specification
- Support for Oracle Service Bus, Microsoft SharePoint, WebSphere, JBoss, and Apache Tomcat
- Enhanced PEP API query requests
- Support for .NET resources
- Administration console support for multiple identity stores.

3. What are the primary usage scenarios for Oracle Enterprise Server?

OES provides a comprehensive and centralized solution for managing access policies with distributed or centralized enforcement. This includes:

- Management and enforcement of fine-grained authorization policies for applications, portals, content, and databases
- Authorization and data redaction for Internet API's, SOA, and Web Services
- Real-time Authorization for Enterprise Applications
- Interoperability and integration through open standards.

4. Can Oracle Enterprise Server be used for real-time authorization in enterprise applications?

OES ensures extremely low latency for mission-critical applications, and is engineered to scale and handle large volumes of sensitive resources, users, roles, and authorization decisions. OES is used in extremely large, mission critical deployments on a wide variety of Oracle and non-Oracle based platforms and solutions.

5. Which Oracle products leverage and use Oracle Enterprise Server for authorization?

OES is Oracle's strategic authorization engine and, out of the box, is embedded in Oracle Fusion Applications, Oracle Fusion Middleware (Oracle SOA Suite, Oracle WebCenter Portal & Spaces, Oracle ADF etc), the Oracle Banking Platform (FlexCube), Oracle Identity and Access Management, and other JRF based applications and technologies. OES also provides integrations with Oracle WebLogic Server and Oracle Service Bus, and can be used in any Oracle WebLogic and Fusion Middleware environment.

6. What authorization models and standards does Oracle Enterprise Server support?

OES supports a large variety of authorization standards and models, including XACML, Attribute Based Access

Control (ABAC), NIST Role Based Access Control (RBAC), "Enterprise" RBAC, Java2 / JAAS Permissions, OpenAZ, and various models for enforcing data security. OES can also act as a Java2 Security Provider and plug directly into the JVM for controlling access to the file system, network and sensitive code.

7. How does Oracle Enterprise Server enable Risk and Context based Access Control?

OES and Oracle Access Management provide a unique end-to-end solution that enables context aware computing. *Identity Context* is automatically made available for authorization decisions by OES, allowing organizations to control what users can do / what information they can access based on the user, device, and runtime context - this includes but is not limited to:

- User attributes, roles, resource and dynamic attributes, environmental conditions
- How did the user authenticate to the system
- What type of device is used to access the system (e.g. a PC, a mobile device)
- Information about the device – is it a registered / trusted device, what is the physical location, IP address, operating system, is it jail broken, is virus scanning and firewall enabled, is VPN enabled etc.
- Assertions from federation partners
- Risk Level – based on real time analysis of anomalies in access patterns and transactions

OES also supports authorization decisions to be based on service context and business context information. The sources of such information are sometimes referred to as policy information points (PIPs). OES uses *Attribute Retrievers* to fetch information about users, resources, or any other information that is used in your authorization policies.

8. What authorization services does Oracle Enterprise Server provide for REST APIs and SOAP based Web Service interfaces?

OES can protect API's, web services, and SOA infrastructures by:

- Blocking or permitting incoming requests based on fine-grained authorization policies
- Perform deep packet inspection of SOAP or REST payloads and selectively permit or deny access based on request content (authorizing business transactions)
- Selectively redact or encrypt sensitive information in the API / web services response

This is often achieved without any changes to the backend web service or SOA application.

OES integrates with API Gateways (e.g. Oracle API Gateway and 3rd party offerings) to secure web services and APIs in the DMZ, and with Oracle or 3rd party ESB's, SOA infrastructure, and a variety of web services in the "Green Zone" (corporate network).

9. What deployment options are available for Oracle Enterprise Server?

The OES authorization engine (PDP) can be either embedded in applications or hosted centrally in the network. Multiple options are also available for policy distribution and caching to meet a wide variety of business, integration, deployment, performance, scalability, and high availability requirements.

10. What ability does Oracle Enterprise Server provide to extend authorization functionality?

Customers can extend functionality using:

- Custom evaluation functions: Customers can write custom java plug-ins, which will be evaluated as part of the policy conditions.
- Custom attribute retrievers: Attributes used in policy conditions can be mapped into custom java plug-ins. Evaluation of an OES policy, which uses these attributes automatically, results in a call to the kava plug-ins. The values returned by the plug-in are assigned to the attribute for policy evaluation.
- User Interface extensions: Organizations can extend the OES Admin Console.

Oracle API Gateway

This section contains frequently asked questions related to Oracle API Gateway (OAG).

General Questions

1. What is the Oracle API Gateway?

Oracle API Gateway" (OAG) is the new name for the "Oracle Enterprise Gateway" product and part of Oracle's Access Management, API Management, Web Services, and SOA security offerings. It is a purpose-built API Security / API Management product offering from Oracle, designed to simplify and secure web services, REST API's, and SOA deployments on-premise, across domain boundaries, and in the cloud. OAG secures, accelerates, integrates, and routes JSON, XML, and other types of data in a simple, easy-to-use manner to help significantly lower integration costs, lower costs of ownership and reduce deployment risks associated with SOA, Cloud, and Mobile infrastructures. It provides the following key capabilities:

API Security and API Management

- Secure Internet APIs and REST/SOAP services against attack and misuse
- Define and enforce API rate limits and SLA metrics
- Content & Context based Routing
- Track and Report on API Usage (Online and Offline)

Secure and Centralized Cloud Connectivity

- SSO for Web and Web Services including SaaS, PaaS, IaaS services
- Secure and Centralized Integration with External SaaS, PaaS, IaaS services
- Manage and monitor Cloud service usage and consumption

Mobile Access Gateway

- Mobile Applications Firewall
- Protocol Bridging and Token/Data Translation (JSON to XML, SOAP to REST, REST to SOAP)
- Data Redaction and Fine-grained Access (in conjunction with Oracle Identity and Access Management)
- Extending Enterprise Identity to Mobile (when used with Oracle Identity and Access Management)

2. Why do organizations need the Oracle API Gateway for Mobile Applications?

Organizations build Mobile Applications to enable anywhere, anytime access for business transactions and information stored in databases, content management systems, and even mainframes somewhere in the corporate network. This information and the types of transactions that users should be able to perform from mobile devices have often only up to this point been available to internal users and applications through client devices issued by the organization – as such these systems often have little, if any, security and compliance controls built in and instead relied on an implied level of trust. Now that we need to expose the corporate systems to devices running outside the corporate network, used by internal and external users, from unknown locations, and over potentially unsecure networks it is critical we do so in a secure way and ensure that we can control what kind of business transactions can be performed and what information leaves our corporate network under what circumstances.

Mobile applications typically access corporate information through lightweight REST based API's as the devices lack support for the more full-fledged application, web services, and SOA based infrastructures based on SOAP, JMS, MQ, or even FTP based technologies that existing corporate systems often are be based on.

Oracle's complete Access Management solution has been designed to help address all these challenges. With the Oracle API Gateway organizations can expose internal systems and corporate data as fully secure REST based API's (using JSON based payloads) without the need for any coding (by virtualizing the existing backend SOAP, JMS etc services as REST API's). Existing transportation protocols and security tokens required for authentication, identity propagation, and user claims (attribute assertions) can be automatically transformed to address modern requirements without changing the existing systems. For example: an organization only want to accept JWT tokens issued by Oracle's Mobile Access Management solution in

their REST API's, but once authenticated the tokens can be converted to SAML, Kerberos, or any other types of tokens that are required by the backend systems.

OAG adds a large number of additional capabilities to an organization's REST API infrastructure – API access, business transactions, and the data requested/returned can be monitored and audited. Requests from mobile clients (or business partners, cloud applications etc) can be validated to ensure they are properly formed, are free from any malicious content and threats such as SQL injection attacks, denial of service attacks (even based on message payload content), viruses, and a large number of other xml, crypto, and other types of attacks.

Throttling policies can be defined to ensure that certain types of clients – perhaps based on their subscription (gold, silver, bronze) – can only perform a given number of transactions per day (or other time interval), charge per usage, and ensure that a rogue client doesn't overload the system with a large number of requests.

Perhaps most importantly the Oracle API Gateway is integrated with Oracle's Access Management technologies – Oracle Access Manager and Access Management Mobile & Social solution for authentication, and validation of user tokens, fraud detection, and Identity Context propagation, Oracle Entitlements Server for authorization and audit of REST API access and selective data redaction of the response payload, Oracle STS for centralized security token management, and also our LDAP directories for user lookup and enrichment of the message payload (adding additional user information from LDAP to the payload).

3. What features does Oracle API Gateway provide as a mobile access gateway?

OAG as a Mobile Access Gateway (working with Oracle Access Management Mobile & Social and other components in Oracle Access Management) provides the following capabilities:

- Protect REST, SOAP and API access against Denial-Of-Service, SQL Injection and API attacks
- Access Control and Identity Integration
- API Key Management
- OAUTH 2.0 Client & Server support
- Content and context based routing
- Mapping between data formats such as XML and JSON and bridging protocols (e.g. REST to SOAP)
- Pre-fetch content and Caching of calls to back-end applications for scalability
- Broker SSO and call-outs to external cloud services
- Recompose and virtualize APIs to specific mobile identities, applications and devices
- Mapping Web SSO and SAML to mobile-friendly OAuth, OpenID Connect and JSON web tokens
- SLA Controls and response caching
- Fine-grained access control and data redaction

4. What are the different API Security and API Management related features provided by Oracle API Gateway?

Threat Protection

- Validate HTTP parameters, REST query/POST parameters, JSON data structures, XML schemas
- Protect against XSS, SQL Injection, XML content/structural threats and viruses
- Create custom threat profiles to extend built- in filters for message structure and XML threats
- Track failed authentications and/or policy violations to identify patterns and potential threats
-

API Key Management

- Assign, suspend and revoke API Keys

Throttling and Quality of Service

- Throttling/rate limiting and quota controls provide control over API traffic

Usage Reporting and Analytics

- Reports that track and meter API usage, successes versus errors
- Real-time Monitoring Dashboard

Access Control

- Support for HTTP basic, digest, SSL certificate based authentication, Microsoft SPNEGO
- Support for SAML, X.509 certificates, LDAP, OAuth
- Authentication against Oracle Access Management

- Fine-grained access control and Data Redaction (working with OES)

5. What is the relationship between the Oracle API Gateway and Oracle Entitlements Server?

OAG is natively integrated with Oracle Entitlements Server to meet the following use cases:

Selective Data Redaction
A large number of organizations across Financial Services, Healthcare, Public Sector / Government Agencies, Telecom, Insurance, and most other industries are looking to expose information and corporate systems to mobile devices, business partners, customers, and the cloud. Many organizations internally expose web services and/or have corporate systems for accessing information about customers, patients, citizens, documents, or other sensitive data. These web services and systems were likely built a long time ago, and often return any and all information about the customer or patient, including sensitive information such as social security numbers, credit card numbers, or medical and health records to the requester. With the combination of OES and OAG, organizations can expose REST based API (or other types of web services) to their clients and define XACML based authorization policies that determine what information should actually be allowed to leave the network or need to be redacted.

Organizations can control what information Bob (for example) can access regarding a given customer or patient from a given client device, location, or network; this automatically redacted information is based on Bob's relationship with the customer/patient (account manager, doctor, something else, or none). In this example, we can determine that the current user should not be allowed to see the customer/patients social security number or date of birth whereas, if Bob were to query a different customer/patient record he would be able to see all the information.

Business Transactions
As in the data redaction example organizations can also control what business transactions a given set of users are allowed to perform under various conditions. This covers not only whether the user is authorized to submit a specific type of business transactions, salary changes as an example, but also for what set of employees, the actual $$$ amount being changed, and under what conditions. Another example could be whether you are allowed to submit orders over a certain amount based on Identity and Device Context.

In both these examples, rules and authorization policies are defined to specify what data can be accessed and whether a given business transaction can be submitted - without any coding or changes required to the backend systems. OAG and OES sit in front of the organizations backend systems and can inspect and control what messages and message content are allowed to go in either direction (request or response).

Organizations gain insight through audit trails and real time as well as offline monitoring of transactions and information flows, and can set up alerts and notifications if anomalies in access patterns and suspicious behavior are detected.

6. How are Oracle API Gateway and Oracle Web Services Manager different?

OAG and OWSM are key components of Oracle's overall layered API and Web Services security solution and provide complementary functionality to provide organizations an end-to-end security solution for their deployments. In an enterprise, API and web services can be implemented using different approaches that need to be secured at the different stages of the request / response cycle between clients (relying parties such as users or applications) and service providers (organizations exposing web services); several security layers are defined between the two. The first security layer in the corporate DMZ ("red zone") is handled by OAG by providing "perimeter security" or the first line of defense. The second security layer (corporate "green zone") is located behind the inner firewall of the DMZ. In some cases, the green zone may include several security sub-layers designed to further filter access to web services. Finally, agents co-located with the web services or applications to be protected provide the last security layer, known as "last-mile security" and handled by OWSM.

7. What support is available in Oracle API Gateway for Microsoft .NET, ADFS and WCF?

OAG interoperates with Active Directory using LDAP, and in the case of ADFS 2.0 (Active Directory Federation Services) it acts as an STS client, consuming tokens from

ADFS 2.0 using WS-Trust. This may be used for scenarios involving single-sign-on with Microsoft SharePoint.

OAG interoperates with all versions of Microsoft .NET services. Interoperability is provided for the WCF (Windows Communication Foundation) policies used by .NET.

8. How is Oracle API Gateway different from Oracle Web Services Manager 10g Gateway?

OWSM 10g Gateway and OAG are two separate products. The OWSM 10g Gateway was discontinued with the release of Fusion Middleware 11g. OAG is Oracle's strategic API Security/Management and DMZ security solution that provides a large number of additional capabilities that were not available in the OWSM 10g Gateway. Refer to the OWSM 10g Gateway to OEG Migration Guide as a starting point for OWSM 10g Gateway to OEG migration.

9. What is the relationship between the Oracle API Gateway and Oracle Service Bus?

The two products complement each other. Oracle Service Bus is generally deployed in the corporate intranet ("green zone") and offer service virtualization, protocol mediation, and heavy duty payload transformation among other things for internal clients and applications. The Oracle API Gateway is generally deployed in the corporate DMZ, also known as the "red zone", and provide a wide array of advanced security capabilities required when exposing API's and web services to the extranet, mobile applications, business partners, and interacting with SaaS, PaaS, IaaS infrastructures. The Oracle API Gateway also offers lightweight service virtualization, protocol transformation, and payload transformation capabilities as this is a requirement for any API Gateway but the primary focus is on capabilities needed in DMZ deployments, such as Threat Protection, Oracle and 3rd party Access Management integrations, client / consumer based throttling, security token mediation, method / API firewalling and blacklisting, Oracle Mobile Access Management integration, API Key Management, Cloud integrations.

10. With which Oracle Identity/Access Management and Middleware products does OAG interoperate/integrate?

OAG is tightly integrated with Oracle Access Manager, Oracle Entitlements Server, Oracle Access Management Mobile & Social, Oracle Directory Services, Oracle Web Services Manager, Oracle Service Registry, Oracle Service Bus, Oracle Business Transaction Monitor, Oracle SOA Suite, Oracle Enterprise Manager Grid Control to provide transport and application-level security across all layers involved in API and web services requests.

11. Is my current investment in the Oracle Enterprise Gateway protected?

Yes, all customers will be able to migrate their OEG licenses to the Oracle API Gateway. Contact your Oracle account team for details.

12. Who should upgrade / migrate to Oracle API Gateway and when?

All OEG customers are strongly recommended to upgrade their deployment to OAG 11gR2 ASAP in order to benefit from new capabilities, performance improvements, and bug fixes. Contact your Oracle account team for details.

Oracle Access Management FAQ 11gR2 (11.1.2.x)
Updated April 2015

Author: Svetlana Kolomeyskaya
Contributing Authors: Marc Chanliau, Venu Shastri, Sid Mishra, Kanishk Mahajan

Oracle Corporation
Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.
Worldwide Inquiries
Phone: +1.650.506.7000
+1.800.ORACLE1
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together